# China: Paper Tiger in Cyberspace

**A Monograph**
**by**
**MAJ Ammilee A. Oliva**
**United States Army**


**School of Advanced Military Studies**
**United States Army Command and General Staff College**
**Fort Leavenworth, Kansas**

**AY 2012-001**

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 03-29-2012 | JUL 2011-MAY 2012 |

**4. TITLE AND SUBTITLE**
China: Paper Tiger in Cyberspace

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**
Major Ammilee A. Oliva, United States Army

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth, KS 66027-2134

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
**Command and General Staff College**
731 McClellan Ave
Fort Leavenworth, KS 66027-2134

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for Public Release; Distribution is Unlimited

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** ***(Maximum 200 Words)***

For the last decade, the PLA has been building its cyber capabilities and expanding the importance of cyber technology military operations. Observers interpret recent cyber incidents as evidence the People's Republic of China (PRC) and the People's Liberation Army (PLA) possess cyber capabilities that pose a threat to the United States and its allies. The question is, are the incidents really manifestations of a PLA threat? To answer that question it was necessary to define cyber attack and cyber war and then determine whether the cyber incidents reported could support the inference that the Chinese have the capability to conduct cyber attacks. Next, it was necessary to interpret Chinese efforts to produce military cyber capabilities and determine if the Chinese possess the intent to attack the United States. Finally, an explanation of hacker incidents assisted in gaining an understanding of the Chinese cyber threat. To constitute a threat an adversary must possess both the capability to attack and the motive. The evidence available shows that the Chinese have made significant technological advances, but their intent to use them against the United States is unclear. China's lack of transparency has caused other nations to speculate and worry about China's intent. Despite PLA interest and preparations for cyber operations, and the importance of networks to military operations, open source evidence does not justify the conclusion that the PRC is a threat per se. Much of what has been classified as a cyber attack is not hostile at all and is actually clandestine spying and a form of intelligence gathering inside computer networks. Hackers, China's internal security threat, are likely their first and foremost priority.

**14. SUBJECT TERMS**
China, PRC, PLA, Cyber Attack, Cyber War, Cyberspace

**15. NUMBER OF PAGES**
35

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| (U) | (U) | (U) | |

# SCHOOL OF ADVANCED MILITARY STUDIES

## MONOGRAPH APPROVAL

MAJ Ammilee A. Oliva

Title of Monograph: China: Paper Tiger in Cyberspace

Approved by:

| | |
|---|---|
| _____<br>William John Gregor, Ph.D. | Monograph Director |
| _____<br>Derek D. Basinger, LCol, (Canadian Army) | Second Reader |
| _____<br>Thomas C. Graves, COL, IN | Director,<br>School of Advanced<br>Military Studies |
| _____<br>Robert F. Baumann, Ph.D. | Director,<br>Graduate Degree<br>Programs |

# Abstract

CHINA: PAPER TIGER IN CYBERSPACE by MAJ Ammilee A. Oliva, United States Army, 35 pages.

For the last decade, the PLA has been building its cyber capabilities and expanding the importance of cyber technology military operations. Observers interpret recent cyber incidents as evidence the People's Republic of China (PRC) and the People's Liberation Army (PLA) possess cyber capabilities that pose a threat to the United States and its allies. The question is, are the incidents really manifestations of a PLA threat? To answer that question it was necessary to define cyber attack and cyber war and then determine whether the cyber incidents reported could support the inference that the Chinese have the capability to conduct cyber attacks. Next, it was necessary to interpret Chinese efforts to produce military cyber capabilities and determine if the Chinese possess the intent to attack the United States. Finally, an explanation of hacker incidents assisted in gaining an understanding of the Chinese cyber threat.

To constitute a threat an adversary must possess both the capability to attack and the motive. The evidence available shows that the Chinese have made significant technological advances, but their intent to use them against the United States is unclear. China's lack of transparency has caused other nations to speculate and worry about China's intent. Defense contractors and politicians have interpreted hacking incidents linked to Chinese citizens to be a manifestation of PRC military activity but the evidence is insubstantial. Despite PLA interest and preparations for cyber operations, and the importance of networks to military operations, open source evidence does not justify the conclusion that the PRC is a threat per se. Much of what has been classified as a cyber attack is not hostile at all and is actually clandestine spying and a form of intelligence gathering inside computer networks. Hackers, China's internal security threat, are likely their first and foremost priority.

# Table of Contents

## Acronyms

| | |
|---|---|
| APT | Advanced Persistent Threat |
| CNA | Computer Network Attack |
| CND | Computer Network Defense |
| CNE | Computer Network Exploitation |
| CNO | Computer Network Operations |
| DoD | Department of Defense |
| EW | Electronic Warfare |
| GSD | General Staff Department |
| INEW | Integrated Network and Electronic Warfare |
| IO | Information Operations |
| IW | Information Warfare |
| JP | Joint Publication |
| NSA | National Security Agency |
| OSD | Office of the Secretary of Defense |
| PLA | People's Liberation Army |
| PRC | People's Republic of China |
| SIGINT | Signals Intelligence |
| TRADOC | Training and Doctrine Command |
| TRB | Technical Reconnaissance Bureau |
| USB | Universal Serial Bus |
| USCYBERCOM | United States Cyber Command |

# Introduction

In January 2010, Google announced it was the victim of a cyber attack originating from China. Further investigation revealed hackers penetrated the networks of over two dozen corporations. Reports alleged China's Politburo ordered the computer attacks and stated the attacks were potentially part of a larger hacking operation executed by individuals hired by the Chinese government. According to one report, the specific purpose of the attack, named Operation Aurora, was to gain access to the Google e-mail accounts of Chinese dissidents and human rights activists and to modify the source code of dozens of high tech security and defense contractor companies. The attackers accessed companies by exploiting vulnerabilities in an Adobe PDF format used in Microsoft's Internet Explorer browser, which enabled the hackers to access a back door, conduct reconnaissance, and gain control over source codes.[1] Conversely, Joel Brenner, former senior counsel at the National Security Agency (NSA), stated the Chinese penetrated Google with the blessing of a member of the Politburo to gain the source code that makes Google unique, not to gain access to e-mail accounts.[2] The assignment of motives to this attack was more speculation than fact because the People's Republic of China (PRC) did not admit to attacking Google, and has never admitted to committing any sort of cybercrime.

In February 2011, the cyber security firm McAfee Inc. announced Chinese hackers made targeted, systematic, and long-term intrusions at five major oil and gas companies resulting in the loss of proprietary information. Investigators named the cyber intrusion Operation Night Dragon. McAfee reportedly had traced the intruder's code back to a server leasing company in Shandong Province, China.[3] The Chinese government did not admit to any involvement in the cyber intrusion.

---

[1] Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2 (Winter 2011): 92-93.

[2] Joel Brenner, "The Calm before the Storm," *Foreign Policy* (September 6, 2011) http://www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm (accessed December 21, 2011).

[3] Desmond Ball, "China's Cyber Warfare Capabilities," 92-93.

Observers interpret these cyber incidents as evidence the People's Republic of China (PRC) and the People's Liberation Army (PLA) possess cyber capabilities that pose a threat to the United States and its allies. Are the incidents really manifestations of a PLA threat? Answering this question is not simple. The question is not simple because to be identified as a threat the adversary must have both the capability and the intent to attack U.S. targets. Unfortunately, determining whether the PLA military activity and hacking incidents constitute evidence of actual cyber attacks is methodologically difficult because there is no agreed upon common definition of either cyber attack or cyber warfare. Additionally, without a clear definition of cyber attack and cyber warfare it is impossible to determine whether the evidence provided by the reported incidents can support the inference that the Chinese possess the capability for cyber attack. Thus, the first step in the research process was to acquire useful definitions of both cyber warfare and cyber attack.

The second issue that needed to be addressed was how to interpret Chinese efforts to produce military cyber capabilities. This was important because an adversary can acquire capabilities related to its security requirements and still not possess the intent to direct cyber attacks at the United States. Consequently, it was necessary to investigate published Chinese cyber related works and cyber activities to determine the extent of those capabilities and to infer from them their intended use. In regard to these two issues, defining cyber warfare proved relatively easy. Emerging U.S. doctrine contains a definition of cyber attack and the RAND Corporation has defined cyber warfare. The merit of these definitions lies in the fact that they are likely to be used by the United States military to make assessments of Chinese actions. Other definitions are available but none of those appear to have influence in U.S. government assessments.

Careful investigation of Chinese cyber doctrine and classification of cyber activities led to the conclusion that the reports of PRC and PLA threats are exaggerated. Much of what serves as evidence of Chinese cyber attacks is actually cyber espionage or evidence of a Chinese hacker community intent on spying or stealing information, rather than disabling systems. Although the Chinese continue to show evidence of advances in cyberspace, such as creation of a cyber blue team, and expansion of the

informatization department within the PLA, these Chinese advances do not constitute evidence of the intention of conducting cyber attacks against the United States. The Chinese government's goal is likely cyber espionage and information theft. Stealing information allows the PRC and PLA to advance technologically at a lower cost.

China's military capabilities are growing but the PRC lacks transparency and does not openly reveal technological advances. The lack of transparency can lead to speculation and worry from other nations regarding China's intent. For the last decade, the PLA has been building their cyber capabilities and expanding the importance of cyber technology in their military. China currently has the world's second-largest economy and has built up their military might across the PLA over the last decade. Former Secretary of Defense Robert Gates, views China as a threat to the United States' national interests and noted China's "investments in cyber and anti-satellite warfare, anti-air and anti-ship weaponry, and ballistic missiles could threaten America's primary way to project power and help allies in the Pacific—in particular our forward air bases and carrier strike groups."[4] Thus, it is evident China has made significant technological advances but their intent to use them against the United States is unclear.

Despite PLA interest and preparations for cyber operations and the importance of networks to military operations, the Chinese do not present a threat per se. Rather research suggests that defense contractors and politicians have interpreted hacking by people within the PRC to be a manifestation of PRC military activity. Moreover, much of what has been classified as a cyber attack is not hostile at all and is actually clandestine spying and a form of intelligence gathering inside computer networks.

## The Problem of Definition

Before one can understand the incidents the media, businesses, and government agencies portray as cyber attacks it is important to define the terms themselves. Terms like cyber warfare and cyber attack

[4]Andrew F. Krepinevich, "The way to respond to China," *Los Angeles Times*, November 9, 2011 www.latimes.com/news/opinion/commentary/la-oe-krepinevich-pacific-20111109,0,3975891.story (accessed November 24, 2011).

are used in the media and even in official Department of Defense (DoD) and government documents but there is no United States military, government, or internationally agreed upon definition of the terms. However, understanding what the United States and China believe constitutes a cyber attack is important for many reasons. First, anyone who uses the Internet is vulnerable. The number of Internet users grows worldwide on a daily basis, which means vulnerability is increasing. Second, the term cyber attack is grossly overused throughout most of the developed world. Almost every day there is a breaking news story on national or international news channels explaining the latest cyber attack. Third, words have meaning and it is important to understand exactly what the term cyber attack means, and its implications to the United States and her allies. Lastly, the United States must work with partner nations to determine common definitions for cyber attack and cyber war as well as determine limits for what is and is not acceptable acts in cyberspace.

Often times the term cyber attack is used when in fact a more appropriate term like cyber espionage, cybercrime or spying should be used. The term cyber attack is an attention getter and often makes the general public think of something physical and scarier than hackers clandestinely breaking through network security and stealing the blueprints on a new fighter jet. Leap frogging expensive technological steps could allow nations like China to develop military equipment like aircraft carriers or satellite technology faster and cheaper. Possessing advanced technologies could allow China to compete militarily with more advanced Western nations like the United States.

To combat cyber threats the United States government and the military invested heavily in standing up the United States Cyber Command (USCYBERCOM). Army General Keith B. Alexander declared the command fully operational capable in October 2010. Subordinate cyber service components are also fully operational. The fiscal year 2012 USCYBERCOM budget is projected to be $159 million

with a total of 464 military personnel and 457 civilians.[5] The mission of this command is to "plan, coordinate, integrate, synchronize, and conduct activities to direct the operations in defense of specified DoD information networks and be prepared, when directed, to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure United States and allied freedom of action in cyberspace, and deny the same to our adversaries." [6] However, the United States Cyber Command is still in its nascent stages and has yet to release the long awaited joint cyberspace doctrine. Current Army doctrine uses the term cyber attack without defining what it means. Army Doctrinal Publication 3-0 *Unified Land Operations* states, "The threat may seek to disrupt U.S. activities through cyber attacks and terrorism in the theater of operations or the United States."[7] Using cyber attack in doctrine without defining it means the term is open to interpretation.

A thorough search of military doctrine and government documents revealed a few broad definitions for the terms cyber warfare and cyber attack. In November 2010, the former Vice Chairman of the Joint Chiefs of Staff released a memo entitled, *Joint Terminology for Cyberspace Operations*. That document defined cyber warfare and cyber attack but so far these definitions have not been incorporated in government and joint military doctrine. The *Department of Defense's Strategy for Operating in Cyberspace* , released in July 2011 is evidence of the dearth of approved definitions. The cyberspace strategy failed to define the terms. None of the joint military doctrine published after Cartwright's memo was released contain definitions for cyber warfare and attack.[8] Despite increased discussions in the media and among politicians regarding the implications of cyber attacks and cyber warfare on the United States

---

[5] Keith B. Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly*, 5, no. 2 (Summer 2011): 4.

[6] Ibid.

[7] U.S. Army Training and Doctrine Command, Army Doctrinal Publication (ADP) 3-0, *Unified Land Operations* (Washington D.C.: Government Printing Office, October 10, 2011), 4.

[8] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* as amended through 15 November 2011 does not list definitions for cyber attack or cyber warfare. However, Joint Publication 3-13 *Information Operations* is obsolete and was last updated 13 February 2006.

in the *Department of Defense's Strategy for Operating in Cyberspace*, the definitions are open for interpretation.

Currently, the closest term in joint military doctrine to cyber attack is computer network operations (CNO). Cartwright's memorandum proposes replacing the term CNO with cyberspace operations but his memo has not stimulated changes to joint doctrine as of early 2012.[9] Joint Publication (JP) 3-13, *Information Operations* explains that computer network operations is the core capability, that encompasses computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE). CNO, along with electronic warfare (EW) "is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure."[10] CNA is broadly defined as being linked to "disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/ networks themselves." [11] CNE is "conducted through the use of computer networks to gather data from target or adversary automated information systems of networks" while JP 1-02 defines CND as "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the DoD information systems and computer networks."[12] From these doctrinal definitions we learn there are several existing doctrinal terms related to cyber attack. Therefore, once military doctrine adopts the term cyber attack these current terms will likely become obsolete.

---

[9]See Vice Chairman of the Joint Chiefs of Staff November 2010 memo entitled *Joint Terminology for Cyberspace Operations*, for more information on the term computer network operations.

[10] U.S. Department of Defense, Joint Publication (JP) 3-13*: Information Operations*, (Washington D.C.: Government Printing Office, February 13, 2006), II-4.

[11]U.S. Department of Defense, Joint Publication (JP) 1-02*: Department of Defense Dictionary of Military and Associated Terms* (Washington D.C.: Government Printing Office, November 15, 2011), 68. See Vice Chairman of the Joint Chiefs of Staff November 2010 memo entitled *Joint Terminology for Cyberspace Operations*, for more information on the differences between cyber attack and computer network attack.

[12]Department of Defense, Joint Publication (JP) 1-02: *Department of Defense Dictionary of Military and Associated Terms*, 68.

With so many casual definitions for cyber attack it is easy to see why determining what is and is not a cyber attack is confusing. In February 2010, the Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-8 indirectly defined cyber attack writing, "cyber attack actions combine CNA with other enabling capabilities (such as, electronic attack, physical attack, and others) to deny or manipulate information and/or infrastructure."[13] The TRADOC Pamphlet 525-7-8 definition of cyber attack does not establish an accepted military definition of cyber attack. Moreover, the definition is so broad that it includes any type of enabling capability in conjunction with CNA. The definition leaves too much room for interpretation, therefore, for the purpose of this study former Vice Chairman of the Joint Chiefs of Staff General (Retired) James Cartwright's definition of cyber attack was selected as the standard.

> A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems of data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure of C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[14]

Throughout this research, Cartwright's definition was used to assess cyber intrusions labeled as cyber attacks by the media and other organizations. Although broad in scope, Cartwright's definition has the virtue that it does not state that exploitation, espionage, or spying are cyber attacks. Acts of CNE will typically go unnoticed by network users and there is no physical harm in stealing secrets.[15] Therefore, this research did not consider acts of exploitation or espionage as cyber attacks.

Additionally, since the United States government does not define cyber warfare; the research sought a definition outside government. RAND's cyber researcher Martin Libicki's defines cyber warfare

---

[13] Army Training and Doctrine Command, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pam 525-7-8, 67.

[14] James Cartwright, "*Joint Terminology for Cyberspace Operations*," November 2010, 5. http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (accessed November 28, 2011).

[15] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Press, 2009), 23.

at the strategic level as "a campaign of cyber attacks launched from one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior."[16] There are various other definitions but most are confusing. For instance, Joel Brenner outlines six different actions that have been called cyber war to include: distributed denial-of-service, electronic propaganda, electronic sabotage, strategic cyber war, operational cyber war, and the criminal terrorist symbiosis. Brenner explains a strategic cyber war would be an electronic war against infrastructure such as railways, air traffic control, or the power grid. He states this type of cyber war has never happened and likely never will. However, he takes a leap and contends all hot wars in the future will be accompanied by operational cyber war, which he argues has happened three times in the past. Brenner contends operational cyber wars took place in 2003 as part of the United States invasion of Iraq because United States military commanders took over Iraq's closed communications system and frightened Iraqi commanders into surrendering. Then, cyber war happened again in 2006 when Israeli fighters flew undetected into Syria to blow up the nuclear weapons facility the North Koreans were building for them. Lastly, an operational cyber war took place in 2008 when Russia invaded Georgia and Russians paralyzed Georgian communications.[17] Apparently, when a term has no set definition, it can be applied to any action involving communications, networks or electronics.

Additionally, it is important to differentiate cyber attacks from other types of cyber intrusions or hacking. In most instances the terms cybercrime, cyber espionage, or denial-of-service describe better the actions that have been classified as cyber attacks. The meaning of the terms cybercrime and cyber espionage vary largely based on perpetrator's intentions and the effects of the act, Cybercrime and cyber espionage are not usually acts the military could counter with equal force. "A cybercrime is activity conducted for profit, primarily motivated by financial gain or notoriety. Cybercrime typically involves the

---

[16]Martin C. Libicki, Cyberdeterrence and Cyberwar, 117.

[17] Joel Brenner, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare (New York: Penguin Press, 2011), 148-153.

production of malware, the distribution of child pornography, hijacking for ransom, the sale of mercenary services, and the like."[18] As stated earlier, cyber espionage is not conducted to cause direct harm but rather to steal sensitive information (i.e. intellectual property). Cyber espionage may be conducted by an individual hacker or an organization and the goal may be monetary gain or a military advantage over an adversary. [19] A denial-of-service attack or distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. A denial-of-service is accomplished by flooding the target with data requests, so that it cannot respond to legitimate traffic, or so that it responds so slowly that it is rendered useless."[20]From this, one concludes that the majority of cyber intrusions are cyber espionage or denial-of-service attacks, and this trend will continue over time.

The last term that needs defining is hacker. However, there are many types of hackers. To keep the term as simple as possible the research defines a hacker as an individual who conducts an illegal act in cyberspace. Therefore, a hacker could commit acts ranging from a denial-of-service to cyber espionage to cybercrime or worse. A hacker is motivated by a myriad of reasons and may work alone, for the government or with a group of activists. It is common knowledge that China has countless hacker organizations within its borders. Many hackers conduct their work as an expression of their nationalistic pride. How do we know that cyber activity originating from China is the work of hackers? Thus, it is important to understand how the United States views events in cyberspace and defines cyber terms. However, the meaning of cyber events and terms do not necessary correspond to those of other nations.

Currently the United States and China both lack widely accepted definitions of cyber war and in both countries, the concept of cyber war is still under development. No credible open source PLA

---

[18]Jonathan A. Ophardt, "Cyberwarfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield", *Duke Law and Technology Review,* February 2010 http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html#B19 (accessed November 25, 2011).

[19]Ibid.

[20] Jason Fritz, "How China will use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala* 8, no. 1 (October 2008): 53.

documents exist that specify what CNO actions against PRC leaders constitute an act of war or what the PLA deems a CNA against an adversary.[21] However, several limited Chinese definitions exist for cyber war. Listed as a type of strategic information operations in the Chinese text, *The Science of Military Strategy*, cyber warfare is defined as "consist[ing] of soft kill (damage or destroy computers and networks) options and is a new operational pattern consisting of attack and protection."[22] This cyber warfare definition is extremely vague and does not provide a clear picture of the extent of damage a cyber war might cause. In this same text cyber attack is translated from Chinese and considered synonymous with information attack.[23]These differences make clear that the United States and China have differing views regarding cyber and information attacks.

In 2005, PLA General Dai Qingmin and his associates wrote an Information Operations (IO) related book entitled *Study Guide for Information Operations Theory*. Dai's book defined computer network warfare indirectly "[Computer] network warfare will act as both a deterrent and a means of warfare, and can have a large and profound impact upon the enemy's politics, economics, and military. It is also an important means of battle for a less well-equipped military against one with formidable strengths in high technology."[24] This broad description of computer network warfare is synonymous with what could be defined as a cyber attack and its potential effects. Dai also wrote, "Whoever controls information and controls networks will have the whole world at his feet."[25] Based on recent Chinese writings it is apparent that continued development and control in cyberspace are extremely important to the PRC.

---

[21] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 7.

[22]Timothy L.Thomas, *Decoding the Virtual Dragon: The Art of War and IW* (Fort Leavenworth, KS: FMSO, 2007), 31.

[23] Ibid.

[24] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance" *Military Review* 88, no.6 (Nov-Dec 2008), 51.

[25] Timothy L.Thomas, *Decoding the Virtual Dragon: The Art of War and IW*, 129.

The United States and the Chinese define cyber terms differently and because of these differences, the disagreement over cyber terms could result in each country misunderstanding the other's intentions. One country may not realize how their actions might be interpreted by the other and those actions may be interpreted as an act of war resulting in deadly retaliation. China uses different terms to discuss cyberspace and often writes about topics such as stratagems to deceive the enemy.[26] The term cyber is not prevalent in Chinese writings and the word they generally use instead is informatization.[27] Informatization is the application of information technology to military operations similar, to how mechanization is linked to the application of industrial technology to military operations.[28] Informatization is China's military strategy to develop completely networked forces throughout all echelons of command and move away from solely focusing on Taiwan to focus on a regionally defensive posture and connect all military operations on land, sea, and air, in space and across the electromagnetic spectrum.[29]

## An Assessment of Evidence against the Definition

DoD is probed everyday by cyber intruders. It is likely the intruders are growing in number and sophistication with every failed attempt. The media is constantly reporting on new cyber attacks and the potential for a future cyber war but says little about what to do about the problem. Regardless of how the cyber threat manifests itself, organizations like the CATO Institute work to maintain a balance between

---

[26]Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," *Cyberpower and National Security*. *Cyberpower and National Security* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: NDU Press, 2009), 65.

[27]Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," *Cyberpower and National Security* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington D.C.: NDU Press, 2009), 465.

[28] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2010," http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf (accessed November 25, 2011) 3.

[29] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 6.

dissemination of information and some degree of government involvement. The CATO Institute is a public policy research institute that believes in individual liberty and limited government. In 2000, David Isenberg, an adjunct scholar at the Institute, said the media exaggerated the cyber threat. Additionally, Isenberg explained that preparing for an actual cyber attack has been a growing industry for years. "Think tanks have been cranking out tomes, and the defense industry has been holding conferences to solemnly announce the emergence of the latest threat." Isenberg sums up his thoughts on the exaggeration of cyber attacks by stating that, "The problem is that we have been inundated by inaccurate and misleading reporting about information warfare—which is usually encapsulated by the phrase, 'Electronic Pearl Harbor.'"[30] The use of the phase 'Electronic Pearl Harbor' is an example of how exaggerated the cyber threat has become.

Additionally, Nigel Inkster states, "China's aggressive activity in cyberspace reads like the script of *Mars Attacks!* It is important to put matters in perspective."[31] Mr. Inkster is currently Director of the International Institute for Strategic Studies in London and was a member of the British Secret Service from 1975 to 2006. Inkster explains that the United States and China have many of the same vulnerabilities in the cyber realm because Western companies developed most of the Internet software. Many Western governments and companies ignored Internet security for years and therefore created exploitable cyber weaknesses for both the West and China. Unfortunately, until the last few years, the Internet market did not place a high demand on security, which is now changing.[32] James Lewis, who has written extensively about the economic costs of a cyber threat from China as well as Russia and Israel, does not believe China would conduct a cyber war against the United States. Moreover, he contends, "From my account there has never been a cyber attack on the United States but episodes of espionage and

---

[30]David Isenberg, "Electronic Pearl Harbor? More Hype than Threat," *Cato Institute Daily* http://www.cato.org/pub_display.php?pub_id=4841 (accessed August 24, 2011).

[31] Nigel Inkster, "China in Cyberspace," *Survival* 52, no.4 (Aug-Sept 2010): 64.

[32] Ibid., 65.

crime."[33] Lewis works as a senior fellow at the Center for Strategic and International Studies and formerly for the Department of State and Commerce. He sees the greatest cyber challenge regarding the Chinese as their ability to freely conduct cyber espionage. Lewis states Chinese officials told him they would never conduct cyber war on the United States because the economic consequences would be too great for China.[34] It is common knowledge that the PRC holds a preponderance of the United States' debt. From this it is reasonable to conclude China does not have an interest in harming the United States' economic system.

In January 2012 an editorial in the *Wall Street Journal* authored by Mike McConnell, Michael Chertoff, and William Lynn confirmed Lewis's statement. The article declares China's cyber thievery is national policy. Additionally, the former director of national intelligence, secretary of homeland security, and deputy secretary of defense state that cyber espionage could have a catastrophic effect on the United States' economy and global competitiveness. The release to Congress of the Office of the National Counterintelligence Executive report in October 2011 confirmed the Chinese government readily practices cyber espionage and confirmed what most open source reports had already made clear, the Chinese government steals information. [35]

Former Director of the National Security Agency, Michael McConnell contends we are constantly fighting a cyber war and losing, but critics say he is exaggerating. McConnell currently works as a cyber contractor. [36] Spying in cyberspace is not war, just as it is not an attack. Military forces conduct

---

[33] Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rule," 2012, 83 http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf (accessed February 11, 2012).

**[34]** Seymour M. Hersh, "The Online Threat. Should we be Worried about a Cyber War?...," *projectworldawareness.com*, December 11, 2011 http://www.projectworldawareness.com/2010/12/the-online-threat-should-we-be-worried-about-a-cyber-war/ (accessed December 23, 2011).

[35] Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery Is National Policy—and Must and Challenged," *The Wall Street Journal*, January 27, 2012.

[36]Mike McConnell, "Mike McConnell on how to Win the Cyber-War we're Losing," *Washington Post.com, February 28, 2010,*

reconnaissance in every military domain. Additionally, exploring the operating environment and setting conditions for future sabotage or operations is something the United States military does under the legal military authorities of Title 10. If an enemy was to plant logic bombs in a computer network, set to go off later it would likely remain undiscovered because cyber defense is so challenging. Therefore, determining whether an act is an intelligence gathering operation or a pre-sabotage act of electronic war is nearly impossible. Joel Brenner states that because acts penetrating military or infrastructure networks are nearly impossible to differentiate they should not be dismissed as "just espionage" because they may be the precursors to an actual act of cyber war in the future.[37]

On the other hand, computer security expert, Bruce Schneier states, "We are not fighting a cyber war now, and the risks of a cyber war are no greater than the risks of a ground invasion. We need peacetime cyber-security, administered within the myriad structure of public and private security institutions we already have." Schneier contends that setting up the cyber infrastructure to thwart acts of hacking and cyber espionage will put the proper infrastructure in place if the United States has to deal with bigger cyber threats in the future.[38] It is likely that a cyber attack that starts a war would not necessarily stay in the cyber realm. Just as land wars in the past have encompassed multiple domains, future wars will grow in sophistication and likely encompass all domains to varying degrees. This means war in the cyber domain may lead to a more traditional looking war fought in the space, air, sea, and land domains.

The current DoD policy regarding retaliation for a cyber attack remains unclear. Only after a definition for cyber attack is accepted by DoD will it be likely to understand what might trigger

---

http://www.washingtonpost.com/wpdyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063 (accessed December 28, 2011).

[37] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 155-156.

[38] Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped," *schneier.com*, July 7, 2010 http://www.schneier.com/essay-320.html (accessed December 23, 2011).

retaliation. “Accordingly, the United States reserves the right, under the law of armed conflict, to respond to serious cyber attacks with an appropriate, proportional and justified military response.”[39] The United States government has not revealed how it plans to identify and retaliate against a cyber enemy. A detailed cyber strategy may never become transparent if it is classified.

Operating effectively in cyberspace is a key element of the President’s 21st century defense strategy. Despite current debate over defense spending cuts, funding for cyber security continues to increase. Because of the increase in DoD cyber security spending defense contractors such as Northrop Grumman, Boeing, BAE Systems, and Lockheed Martin are buying up cyber security firms in order to compete for government dollars.[40] The Pentagon stated that they are requesting $3.2 billion for cyber security in fiscal year 2012. Cyber security, like cyber attack or cyber war, is a very broad term and has the potential to be redundant.[41]Therefore, it is difficult to determine what DoD will spend cyber security funds on because there is a definite overlap between areas such as information assurance and operations security. However, having a transparent cyber strategy would like it more likely that the United States government will develop a comprehensive plan to allocate cyber funding.

Depending on the rate and intensity of future cyber attacks, the cyber security business may remain lucrative for years to come. Nevertheless, with an ever-evolving cyber threat, defense contractors will have to work extremely hard to maintain their position in a competitive market. The non-profit research group, TechAmerica Foundation, predicts the United States will spend $10.5 billion on cyber security by 2016 if small cyber attacks continue against the country and up to $13 billion if there is a large

---

[39]William J. Lynn III, “The Pentagon’s Cyberstrategy, One Year Later” *Foreign Affairs.com*, September 28, 2011. http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons- cyberstrategy-one-year-later (accessed September 30, 2011).

[40]“DoD Cybersecurity Spending: Where is the Beef?,” *defenseindustrydaily.com*, June 14, 2011 www.defenseindustrydaily.com/cyber-security-department-defense-spending-06882/ (accessed September 29, 2011).

[41]Ibid.

cyber attack.[42] However, in a Forbes.com blog, Loren Thompson stated, "cyber warfare isn't like other market segments — it is in flux, and may remain that way for a long time to come. That means even if government spending on cyber warfare keeps growing, some players straining to get into the business are not going to be happy with how this new opportunity works out."[43] Thompson is Chief Operating Officer of the non-profit Lexington Institute, which receives money from many of the nation's leading defense contractors.

Despite the worry that the United States is not doing enough to thwart attacks and lacks the skill to keep up with technology, defense spending is through the roof. Currently the United States defense spending is greater than the next ten countries combined. China is the second largest defense spender in and the United States is still spending six times more than China.[44] China has achieved tremendous military growth over the last decade and by sheer numbers has the largest military in the world. However, despite China's huge increase (percentage wise) in spending since 2001, and the fact that China has missiles that could range the United States, China is still far behind the United States militarily.

## Interpretation of Chinese Military Cyber Activities

To understand the PLA and how they view the development of their capabilities in cyberspace it is necessary to have a rudimentary understanding of Eastern military theory. The Chinese have historically used an indirect approach in war. Sun Tzu is perhaps the oldest and best known of all Eastern military theorists, although no one is sure who he really was.[45] His dictums are held in high regard today

---

[42]"DoD could spend $13 billion on cybersecurity by fiscal year 2016,"*infosecurity.com*, October 20, 2011 http://www.infosecurity-magazine.com/view/21488/dod-could-spend-13-billion-on-cybersecurity-by-fiscal-year-2016/ (accessed October 29, 2011).

[43]Loren Thompson, "Cyberwarfare May be a Bust for Many Defense Contractors," *forbes.com*, May 9, 2011 www.forbes.com/sites/beltway/2011/05/09-washingtons-cyberwarfare-boom-loses-its-allure/ (accessed October 29, 2011).

[44] "Background paper on SIPRI military expenditure data, 2010," *Stockholm International Peace Research Institute*, April 11, 2011, 1. www.sipri.org/research/armaments/milex/factsheet2010 (accessed January 22, 2012).

[45] Henry Kissinger, *On China* (New York: Penguin Press, 2011), 25.

in Eastern thought and studied throughout militaries all over the world. Similar to Carl von Clausewitz and his enduring influence on the "Western Way of War," Sun Tzu's way of thinking can be adapted to fit any type of warfare from nuclear to cyber. Sun Tzu taught the art of deception, the ability to appear strong when you are weak and weak when you are strong, and to "offer the enemy bait to lure him; feign disorder and strike him."[46] What distinguishes Sun Tzu from Western military strategists is his emphasis, not just on the military aspect of war, but on the psychological and political elements as well.[47]

The Western tradition of war emphasizes the clash of forces and acts of heroism while the East values subtlety, indirectness, and patience in order to accumulate relative advantage over the adversary to potentially win without ever fighting.[48] Andrew Krepinevich, President of the Center for Strategic and Budgetary Assessments, an independent policy research institute, stated in an editorial in the *Los Angeles Times* that writing in military journals strongly indicates the PLA sees America as their principle rival. However, China's ultimate goal may not be to wage war, but to shift the balance of power to China's favor to a point where Washington no longer has the ability to defend its interests or its allies. If this happened, China would succeed in defeating the enemy before the first battle.[49]

The idea of defeating the enemy before the first battle is in line with Sun Tzu's concept of *shih* or strategic advantage. Strategic advantage is a combination of surprise and straightforward operations in battle. In battle, the straightforward aspect of war is used to engage the enemy, and surprise, to win. For example, the perfect timing of a drawn crossbow hitting its victim at precisely the right moment or a bird attacking and smashing its prey into pieces on the rocks demonstrates *shih*.[50]

---

[46] Sun Tzu, *Sun Tzu: The Art of Warfare*, ed. and trans. Samuel B. Griffith, (New York: Oxford University Press, 1971), 66.

[47] Henry Kissinger, *On China*, 26.

[48] Ibid., 23.

[49] Andrew Krepinevich, "The Way to Respond to China," *Los Angeles Times*, November 11, 2011 http://articles.latimes.com/2011/nov/09/opinion/la-oe-krepinevich-pacific-20111109 (accessed November 12, 2011).

[50] Sun Tzu, *Sun Tzu: The Art of Warfare*, 119-121.

To support the Chinese concept of seizing the initiative by exploiting surprise, the Chinese developed a set of military capabilities called the Assassin's Mace or Chinese, *Shashoujian* to explain this strategic philosophy. The Assassin's Mace could potentially be used to threaten the United States and her allies, and interests in the Far East. The military capabilities associated with the Assassin's Mace are advanced air defense, information warfare, advanced fighter aircraft, attack submarines, ballistic and cruise missiles, as well as counterspace capabilities. These are all areas the PLA has been working to modernize or develop over the last ten years after the United States military demonstrated its military prowess in the Gulf War, against an enemy using predominately Chinese weapon systems.[51]

Historically the PLA based its military rules and regulations on a way of fighting based on using an active defense. Active defense meant China would not strike first but would be ready to respond if attacked. This strategic policy changed incident to the birth of the cyber era. Current open source PLA writings discuss the importance and need for offensive operations. This change in strategy reflects a clear shift from traditional defensive-minded military thinking to an offensive mentality.[52] "Information technology has thus stimulated Chinese strategic thinking; military academics now argue that those who do not preempt will lose the initiative in what may be a very short lived IO war."[53] According to the November 2011, *US-China Economic and Security Review Commission*, the PLA seeks to defeat a technologically superior opponent, and their military strategy emphasizes striking first and controlling China's border in the event of a conflict.[54]China's shift from a defensive to an offensive strategy means China wants the ability to strike first and maintain the offensive when necessary.

---

[51] Andrew Krepinevich, *7 Deadly Scenarios: A Military Futurist Explores War in the 21st* Century (New York: Random House, 2009), 185-89.

[52] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance" *Military Review* 88, no.6 (Nov-Dec 2008): 48.

[53] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance," 49.

[54] Carolyn Bartholomew, *2011 Report to Congress of the US- China Economic and Security Review Commission*, (Washington, DC: Government Printing Office, November 2011), 18.

After gaining an idea of how the PLA is thinking, it is important to understand the PLA's structure. The PLA maintains at least six regionally based Technical Reconnaissance Bureaus (TRB), that are believed to be subordinate to the Third General Staff Department. The Third Department is responsible for ensuring the security of the PLA computer systems to keep foreign enemies from accessing sensitive national security information.[55] It is also likely the Third Department is responsible for providing policy guidance and assigning collection and analysis tasks to the TRBs.[56] The TRBs' mission is signals intelligence (SIGINT) collection against tactical and strategic targets and computer network operations. However, no detailed open source data exists on these bureaus. Moreover, no clear evidence exists showing when these six TRBs were created or how they have evolved. However, in 2002, the Third TRB received a fifth consecutive annual award for its outstanding "research in information warfare theories." It is possible this particular TRB has existed and has been conducting an information warfare mission from as early as 1997.[57]

In 2003, the PLA announced it would activate the first high-tech Information Warfare (IW) units in Beijing. The IW units possess capabilities for network warfare on the Internet and have the ability to transfer data using remote sensing satellites. In addition, around 2003, the Chinese military began publishing books and articles focusing on the importance of IW, military informatization, digitization, and movement from the mechanized age to the information age. One of the more influential Chinese military writers was General Dai Qingmin. Dai wrote about the six forms of IW to include: deception, intelligence, physical destruction, electronic warfare (EW), operational security, and computer network

---

[55] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute*, November 11, 2011, 3. https://project2049.net/publications.html (accessed November 15, 2011).

[56] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute*, 6.

[57] Carolyn Bartholomew, *2011 Report to Congress of the US–China Economic and Security Review Commission*, 32.

attack. Based on these rough timelines it is fair to conclude that the PLA have been focusing on cyberspace for at least a decade.

General Dai also discussed the concept of integrated network-electronic warfare (INEW), which is similar in concept to the United States idea of network centric warfare. INEW combines the offensive missions of CNA and EW together. In the PLA's General Staff the Fourth Department (Informatization) is responsible for INEW.[58] The Computer Network Defense mission was given to the PLA's General Staff Third Department (SIGINT) along with intelligence collection responsibilities.[59] Dai's writings insisted the Chinese military must move away from just electronic warfare to include network operations as represented in INEW and IO must include both offensive and defensive IO equipment.[60] Dai stated, "It is important to take the initiative and effectively destroy the enemy's electronic information systems."[61] In the PLA, theory guides training. Doctrine is developed later based on an evaluation of the training. To practice the INEW plan and attack the enemy at critical weak points, grasp key junctures, or seize the commanding high ground, the PLA may have developed an opposing force to simulate the enemy and provide training for the PLA.[62]

The Office of the Secretary of Defense (OSD) stated that in 2009, many computer systems owned by the United States government were targets of cyber intrusions traced to the PRC. Utilizing the same skills that would be necessary to conduct computer network attack, these perpetrators stole information with strategic or military value. OSD does not know if these intrusions were government sponsored but

---

[58] Zhang Yanzhong and Li Qiang, "GSH Communication Department Restructured into an Informatization Department," *Jiefangiun Bao*, July 1, 2011.

[59] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation (October 9, 2009) http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed November 25, 2011), 7.

[60] Timothy L. Thomas, *Dragon Bytes: Chinese Information War Theory and Practice* (Fort Leavenworth, KS: FMSO, 2004), 56-59.

[61] Timothy L. Thomas, *Dragon Bytes: Chinese Information War Theory and Practice*, 58.

[62] Ibid., 58-59.

claims the skills involved show evidence of the developing capabilities consistent with PLA military writings.[63] According to OSD, the PLA's IW militias developed viruses capable of attacking enemy computer networks as well as tactics and measures necessary to protect friendly computer systems and networks. These units include militia elements that now create a link between PLA network operators and China's civilian information technology professionals. The PLA can now combine EW and CNO to deny enemies access to information necessary to conduct combat operations.[64]

OSD reports that the PLA is working hard to develop offensive cyber warfare capabilities but has given little thought to the global and systemic effects that the use of this strategic capability would pose.[65] In May 2011, the Chinese Defence Ministry announced the PLA stood up a 30 person Blue Army of cyberwarriors dedicated to providing Internet security and defending China's computer networks. The unit was created from an exceptionally deep talent pool but the spokesperson from the Chinese Defence Minister's Office claims the unit will only be used for defense.[66] According to Desmond Ball, a professor of Strategic and Defence Studies Centre at the Australian University, the PLA has not demonstrated the ability that they can do more than conduct rudimentary offensive cyber warfare. Additionally, China's cyberwarriors have not demonstrated they have the ability to penetrate highly secure networks or covertly steal or falsify critical information.[67] However, instead of planning on assumptions that the PRC is unprepared to conduct a cyber attack or worse, cyber war, it is imperative the United States government takes the required steps to ensure the nation is protected. Consequently, if the United States does not have

---

[63] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2010," (2010), 7, http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf (accessed November 26, 2011) .

[64] Ibid., 37.

[65] Ibid., 34.

[66] Leo Lewis, "China's Blue Army of 30 Computer Experts could Deploy Cyber Warfare on Foreign Powers," *The Times*, (May 27, 2011) http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826 (accessed December 2, 2011).

[67] Desmond Ball, 101.

a clear idea of what the Chinese government is capable of doing in the cyber domain they should plan to conduct offensive and defensive cyber against several different scenarios.

The Chinese government denies its involvement in cyber attacks and the PRC claims they are a victim just like everyone else. However, a United States Government commissioned report by United States defense contractor, Northrop Grumman, reported, "The PLA is reaching out across a wide swath of the Chinese civilian sector to meet the intensive personnel requirements necessary to support its burgeoning information warfare capabilities."[68] China's population has the highest percentage of Internet users in the world. Thus, it is logical China has a high volume of internal cyber threats as well as external threats.

Two recent cyber studies show that China's ability to project cyber power and maintain cyber security are far behind the United States and other western countries. United States defense contractor, Booz Allen Hamilton's cyber power index ranks China number 13 for cyber power out of the 19 G20 countries (the EU is excluded). Booz Allen Hamilton defines cyber power "as the ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy." [69] Despite being the second largest defense spender in the world, China's ability to defend itself against cyber attacks and to maintain sound cyber infrastructure is below average compared to other technologically developed nations. China is ranked between Argentina and Russia. The United States, United Kingdom, and Germany occupy the top spots in the study's findings.[70] Additionally, the Brussels-based Security and Defence Agenda groups China in the third of five tiers denoting cyber security

---

[68] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *Northrop Grumman Corporation*, October 9, 2009 http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed November 25, 2011), 7.

[69] Economist Intelligence Unit, Booz Allen Hamilton, *Cyber Power Index: Findings and Methodology* 2011, 2-4. http://www.cyberhub.com/Home/DownloadFindings (accessed February 11, 2012).

[70] Ibid., 4.

readiness.[71] The United States and the United Kingdom were ranked in the fourth tier while no countries were ranked in the top or fifth tier.[72] Although these reports are subjective, they indicate China is not as prepared in cyber as leading western countries. Truly understanding China's cyber readiness is difficult because they lack transparency, which means their level of cyber sophistication, and how they weight their efforts is unclear.

Why is there such a disparity in opinions when it comes to understanding the PLA's cyber capabilities? Many security experts contend the PLA is a legitimate cyber threat to the United States, whereas other cyber and intelligence experts discount the idea and believe that to date very few cyber attacks have happened and that a cyber war has never happened.[73] Whatever one's stance, cyber attacks have been the subject of increasing public attention. Deputy Secretary of Defense William Lynn argues, "The United States must guard against both a cyber "Pearl Harbor," as Secretary of Defense Leon Panetta has warned, and the possibility of a cyber 9/11."[74] However exaggerated this claim, poor information security is a problem the government and corporations need to address. Without taking the proper precautions to ensure the safety of computer networks the networks are vulnerable to anyone with some computer science knowledge and the desire to buy a hacking tool kit from the Internet.

In a January 2010 *Foreign Policy* article, journalist Josh Rogin described 10 cyber incidents commonly cited in the news and in security agency and government briefings as evidence that the Chinese are indeed linked to cybercrimes against the United States. His article stated China was the

---

[71] Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rule," 2012, 55. http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf (accessed February 11, 2012).

[72] Ibid., 80-83.

[73]William Jackson, "When is a Cyberattack not a Cyberattack? Most of the Time." *Federal Computer Week* August 8, 2011, 30.

[74]William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later," *foreignaffairs.com* September 28, 2011 http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later?page=show (accessed September 30, 2011).

perpetrator in all of the intrusions but the article did not explain how that was determined. Listed below are four significant cyber intrusions said to have originated from China.

> In 2004, Titan Rain was the Federal Bureau of Investigation's name for a massive cyber espionage ring linked to government sponsored hackers in the Guangdong Province in China. The hackers were responsible for stealing information from the military and the United States. government over a period of years. The hackers stole information from military labs, National Aeronautics and Space Administration, the World Bank, and other institutions.[75] Like many of these cyber intrusions, it is unknown whether Chinese security agencies committed the intrusions or if hackers chose to mask their identity by using China-based computers. Additionally, stealing information from institutions is not considered a cyber attack as Cartwright insinuated in his definition of cyber attack.
>
> In August 2006, Representative Frank Wolf, an outspoken lawmaker on Chinese human rights issues, announced his office computers, those of several other congressional Representatives, and the office of the House Foreign Affairs Committee were compromised. Wolf said he suspected the Chinese.[76] Again, the Chinese are blamed but without explanation. Are they just an easy scapegoat for Western society and our allies? Probing a computer network's security defenses, viewing, and copying information has never been considered a hostile act as required by Cartwright's definition.
>
> In December 2006, the Naval War College took all of their computer systems offline for weeks following a major systems attack traced back to the Chinese.[77] Although the Navy suspected the Chinese, no United States official confirmed that the attacks at the Naval War College had Chinese involvement at the government level.[78]
>
> In March 2009, Toronto based researchers revealed the results of a 10-month investigation they named Ghostnet. The researcher's findings confirmed over 1,200 systems in 103 countries were victims of a cyber espionage ring using Chinese malware from Beijing. Victims of the cyber espionage included foreign embassies, non-government organizations, news media outlets, foreign affairs ministries, and international organizations. The research also indicated almost all Tibet-related organizations and the offices of the Dalai Lama were victims.[79] This massive intrusion appears to have originated from China but Russia also looked like it was responsible for hacking into Estonia. All four of these examples of cyber intrusions reveal acts of cyber espionage rather than cyber attacks. Moreover, it is unknown if the Chinese government was responsible.

---

[75] Josh Rogin, "The Top Ten Chinese Cyber Attacks that we Know of," January 22, 2010. http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of (accessed November 24, 2011).

[76] Ibid.

[77] Ibid.

[78] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," 467.

[79] Josh Rogin, "The Top Ten Chinese Cyber Attacks that we Know of."

Regardless of whether China is the perpetrator, according to McAfee, everyone is a victim of a cyber intrusion. In fact, every company in every type of industry with significant size and valuable intellectual property and trade secrets has been a victim of a cyber intrusion or will be in the near future. McAfee's former Vice President, Dmitri Alperovitch made this allegation in 2011 following investigations on Operation Aurora and Operation Night Dragon (cyber intrusions discussed in the introduction) and other intrusions from companies who have not come forth publically. McAfee also stated that the majority of the victims rarely discover the intrusion's impact. Alperovitch divides the Fortune Global 2,000 firms into two categories: those that know they have been compromised and those who have not discovered it yet. McAfee's *Operation Shady RAT* report released in mid-2011, does not name the actor or group responsible for the cyber espionage operation that affected 14 countries and 71 targets.[80] However, following the release of this report, Reuters and other national news agencies pointed to China over Russia as the likely threat responsible for this large-scale operation.[81]According to General Cartwright a cyber attack is a hostile attack. If a cyber intrusion can go completely unnoticed, it is not a cyber attack as some companies and politicians claim. A hostile attack is violent or destructive.

Until approximately five years ago, many of the reported cyber intrusions were limited in scope and were financially motivated. McAfee's long-term research on cyber intrusions demonstrates that any organization can become a victim: the United Nations, a multinational Fortune 100 company, a small, non-profit think tank, a national Olympic team, or a computer security firm. McAfee is most concerned with Advanced Persistent Threats (APTs) attacking companies and governments to steal secrets and private information over a long-term. The Stuxnet virus was eventually labeled an APT but to earn that title an intrusion must show the following qualities: it must be purpose driven and tailored to infect

---

[80]Dmitri Alperovitch, "Revealed: Operation Shady RAT".

[81] Jim Finkle, "State Actor" behind Slew of Cyber Attacks," *Reuters.com*, August 3, 2011, http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803 (accessed December 20, 2011).

specific targets, use a slow infiltration technique, have organized and well-funded perpetrators, and use various and concurrent attack approaches.[82] APTs are stealthy and can remain in a system undetected for long periods before going active. The Stuxnet virus attacked centrifuges in Iran causing a long term set back in their uranium enrichment program and their ability to develop nuclear weapons. This means at least one nation possesses the money and technical expertise to develop an APT.

Many so-called cyber attacks are attributed to China, but the Chinese government never admits guilt and according to unclassified research, a direct link to the Chinese government is only speculation. However, in July 2011, a six-second long video from a Chinese state media documentary called, "The Cyber Storm Has Arrived," depicted a denial-of-service attack against a Falun Gong organization's website. The video showed the attackers selecting an attack mode from a drop down menu of options. Western experts who viewed the video clip said the military computer program featured in the clip was not very sophisticated and probably does not represent the extent of PLA offensive cyber capabilities. However, experts were intrigued by the fact that this was the first time the PLA was showing off cyber capabilities and demonstrating their intention to conduct a denial-of-service attack on their internal enemies. In this case, the adversaries, Falun Gong, were working off computer servers in another country and the IP address attacked was linked to the University of Alabama in Birmingham. "Based on Internet Protocol data exposed in the program and information from the school's network administrators, the attack appears to have taken place in 2001 or earlier."[83] A Falun Gong spokesman said he knew China was working for years to hack into their systems but had no idea military resources were involved. [84] It is

---

[82] John Zyskowski, "Advanced persistent threats: Be fearful but keep perspective," *Federal Computer Week,* August 8, 2011, 28.

[83] Carolyn Bartholomew, *2011 Report to Congress of the US–China Economic and Security Review Commission*, 177.

[84] Ellen Nakashima and William Wan, "China's Denial about Cyberattacks undermined by video clip," The Washington Post (August 22, 2011) http://www.washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html (accessed on August 25, 2011)

likely the denial-of-service on the now defunct Falun Gong website was a decade old and yields no conclusive evidence of current PLA cyber capabilities.

In 1999, Falun Gong was banned in China and the government began a decade long crackdown on the organization it viewed as an "evil cult." Most objective Western scholars classify Falun Gong as a new religious movement.[85] Many Falun Gong leaders and followers have been killed or imprisoned over the years and the Chinese government censors their websites and blocks public access to Falun Gong material.[86] Even back in 1999, Falun Gong demonstrated an uncanny ability to organize 10,000 protestors for a sit-in demanding an end to criticism of the organization.[87] With access to today's social networking technology it might be more difficult for the Chinese government to interfere with Falun Gong communications. Overall, the recent release of an old example of a cyber intrusion on an anti-PRC organization does little to advance the credibility of the claim that the PLA maintains a highly sophisticated cyber capability.

More notable cyber attacks in 2010 did not involve implanting malicious code or viruses but required human assistance on the inside. Two of the most notable cyber threats of 2010 noted in the 2011 *Symantec Internet Security Threat Report* were Stuxnet and Hydraq. According to Symantec's investigation and subsequent reporting on the Stuxnet virus, although they cannot definitively say who was responsible for the attack, it was evident it could not have breached its target without someone on the inside with access to a universal serial bus (USB) key. Additionally, Hydraq (also known as Operation Aurora) would not have been successful if the code had not convinced network users that the Trojan was

---

[85] David Ownby, "The Falun Gong in the New World," *European Journal of East Asian Studies* 2, no. 2 (2003): 303.

[86] Ellen Nakashima and William Wan, "China's Denial about Cyberattacks undermined by video clip," *Washington Post*, August 22, 2011, http://www.washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html (accessed on August 25, 2011).

[87] Jeffrey N. Wasserstrom, *China in the 21st Century: What Everyone Needs to Know*, 81.

sent via e-mail from a trusted source so that users willingly opened the links and attachments.[88] If computer users were more wary of network threats and more skilled in employing enhanced anti-virus software it is possible these cyber intrusions might not have spread or have been less severe.

The PLA hides its modernization efforts. According to the Northrup Grumman report, "official statements from Beijing over the past year describe China as a status quo power and downplay its military modernization efforts."[89] China's lack of transparency creates problems both externally and internally. Externally the western world does not have a clear picture of China's intentions. Internally the PRC keeps a close eye on its population. The PRC censors material and controls access to cyberspace creating animosity among China's youth. If so-called Chinese Netizens want to figure out workarounds to access the web free of censorship it pays to learn how to hack the government required software. Therefore, loathing toward the government and the easy acquisition of hacker software from the Internet gives China's youth incentive to learn how to use hacking tools.

## Interpretation of Hacking Incidents and an Explanation

With the unique nature of networks, anyone with the right tools can be a hacker, spoof their location, and cover up their tracks to leave no trace that they were involved. This low-cost, low-risk way of conducting cyber attacks adds to the appeal. Understanding the tools hackers used as well as their sophisticated techniques is beyond the scope of this research. However, China's efforts to control their technically competent youth preoccupy limited PRC investigative resources. Tang Lan and Zhang Xin of the East West Institute contend, "China's crackdown on hacker activity is truly needed to protect national

[88] Symantec Corporation, *Symantec Internet Security Threat Report: Trends for 2010*, 16 no. 1, (April 2011): 4, https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf (accessed December 26, 2011).

[89] Carolyn Bartholomew, *2011 Report to Congress of the US–China Economic and Security Review Commission*, 180.

interests; it is by no means done 'for show,' as the Western media has charged."[90] This means China is more distracted stopping their internal cyber threat than many Western nations probably realize.

According to Northrop Grumman's 2009 report, "Little evidence exists in open sources to establish firm ties between the PLA and China's hacker community, however, research did uncover a limited number of cases in which more elite individual hackers collaborated with the PRC's civilian security services."[91] However, any detailed information regarding these links is extremely limited and it is difficult to verify these relationships. Moreover, over the last few years the Chinese government has attempted to show they do not condone hacker attacks. In February 2009, the Chinese National People's Congress expanded China's anti-hacking law and made some high profile arrests against hackers to demonstrate their seriousness towards prosecuting hackers. As of 2009, China's anti-hacking law prohibits hacking into the PRC government computer system and criminalizes the creation and distribution of malicious software.[92]

The Chinese government has internal and external cyber targets. Internally, Chinese citizens are constantly under surveillance. The leadership in China struggles to censor and limit the sharing and viewing of information on the World Wide Web. To maintain control of organized hackers, China attempts to organize their government cyber warfighters into a chain-of-command. The government imposes punishments and regulations against those failing to comply with cyber restrictions. Chinese leadership is working diligently to constrain and contain citizens from openly using the Internet to gain

---

[90]Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" *Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway*, Edited by Andrew Nagorski, East West Institute, April 2010 www.ewi.info/system/files/CyberDeterrenceWeb.pdf (accessed on December 24, 2011), 2.

[91] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, 7.

[92] Ibid., 39.

sensitive information.[93] However, there are ways to circumvent the Great Fire Wall which involve using proxy servers and VPNs (virtual private networks), tools which can make it appear as though the user is somewhere other than China.[94] Therefore, it is difficult for the Chinese government to identify and target perpetrators of hacking attacks.

In 2009, Symantec's *Global Internet Security Threat Report* noted that 7 percent of Internet attacks originate from computers in China, that was a decrease from 13 percent in 2008.[95] The Symantec Corporation is a government vendor for network security. However, their statistics clearly showed China a distant second to the United States, as the place of origin for web-based attacks. Chinese officials pointed out in January 2010 that they are the biggest victim of hacking attacks worldwide.[96] According to Symantec, China ranks second in the world next to the United States for malicious computer activity.[97] China has a difficult time keeping their nationalistic hackers from interfering with domestic government networks. According to cyber expert, James Lewis, the Chinese are far more interested in domestic control and regime survival than they are in external efforts against competitors like the United States.[98]

If the PRC fails to thwart hacker intrusions, hackers may make it appear as though the PRC is conducting a cyber attack on another state when in fact the hackers are the source. In 2007, data from an attack on the Estonian government and private infrastructure appeared to originate in 178 different

---

[93]Edward Timperlake, "Testimony on Cyber-attacks, Espionage, and Technology Transfers to the People's Republic of China," *Foreign Affairs Committee, United States House of Representatives*, published April 15, 2011 http://www.strategycenter.net/research/pubID.242/pub_detail.asp (accessed November 25, 2011).

[94] Jeffrey N. Wasserstrom, *China in the 21st Century: What Everyone Needs to Know* (New York: Oxford University Press, 2010), 86.

[95] Symantec Corporation, "Symantec Global Internet Security Threat Report Trends for 2009", 15, no.1, (April 2010), 25. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (accessed December 26, 2011).

[96]"Accusation of Chinese Government's Participation in Cyber Attack "Groundless": ministry," *Xinhuanet.com* January 25, 2010 http://news.xinhuanet.com/english2010/china/2010-01/25/c13149276.htm (accessed December 21, 2011).

[97] Symantec Corporation, "Symantec Global Internet Security Threat Report Trends for 2009", 19.

[98] Desmond Ball, "China's Cyber Warfare Capabilities," 100.

countries. However, the Russian government was seen as having the greatest motive and was, therefore, blamed for the attack until two years later when a Russian youth group admitted responsibility.[99] Incidents such as this one demonstrate the importance of being able to effectively trace a cyber attack back to the perpetrator. Currently, there is nothing to keep a non-state actor from appearing to be a nation-state in order to manipulate another country into responding to a cyber attack. Retaliating for a cyber attack could have devastating consequences if the actual perpetrator is not determined prior to responding.[100]

Over the last 10 years, a myriad of cyber intrusions have been detected and traced to IP addresses in China. Additionally, individuals like Alan Paller, research director of the security training firm SANS Institute, believes the Chinese cyber threat is growing. The SANS Institute located in Bethesda, Maryland, offers a cyber security graduate degree with security classes ranging from basic operations security to advanced hacking techniques. According to Paller, the cyber security problem is 1,000 times greater than what is visible.[101]The media, like Paller, make the cyber threat appear more aggressive over time. However, an increasing over reliance on the Internet logically means there are more vulnerable victims available. According to Ting Xu, Senior Project Manager at the Washington, D.C. based Bertelsmann Foundation, research shows that 80 percent of the global cyber incidents are economic crimes and motivated by profit.[102] Which means only a small percentage of cyber incidents are politically or militarily motivated. Understanding and distinguishing between different types of motives is vital to help understand the threat.[103]

---

[99] Ting Xu, "China and the United States: Hacking Away at Cyber Warfare," *Asia Pacific Bulletin* 135 (November 1, 2011), 1. http://www.eastwestcenter.org/publications/china-and-united-states-hacking-away-cyber-warfare (accessed December 27, 2011).

[100] Ting Xu, "China and the United States: Hacking Away at Cyber Warfare," *Asia Pacific Bulletin*, 2.

[101]Josh Rogin, "The Top Ten Chinese Cyber Attacks that we Know of."

[102] The Bertelsmann Foundation is German's largest private non-profit organization active in active in political, social, economic, educational, cultural and health-related issues.

[103] Ting Xu, "China and the United States: Hacking Away at Cyber Warfare," *Asia Pacific Bulletin*, 1.

Worldwide media reports constantly blame China for commercial espionage or cyber attacks. However, if Chinese hackers are to blame, there are many groups in China that may be responsible for the cyber intrusions. Each group may or may not be driven to act by the PRC or the PLA. Unclassified literature accusing China of cyber attacks typically fails to differentiate between the PLA's General Staff Department Third and Fourth Departments, the PLA's Information Warfare militias, or young nationalistic hackers. These groups likely have very different motives for conducting cyber intrusions ranging from planting malware into a network to disabling a network. Although various Chinese groups possess the ability to conduct cyber intrusions their motive and ability to conduct cyber attacks on the United States can be difficult to ascertain.

Security analysts and defense contractors assert that cyber intrusions typically originate from servers in China. However, they cannot determine if the hackers are legitimately located in China. Bruce Schneier, the founder and chief technology officer of BT Managed Security Solutions, an Internet security company in the United States, explains the connection between a large number of hackers and their link to China. He contends it is not likely they are in X country and trying to appear that they are in China, but are a bunch of young patriotic Chinese men who want to show off their hacking skills. Most likely, these young men are not linked to the Chinese government. Conversely, they are part of the bored and technologically advanced youth bulge existing in China. Schneider contends, "The hackers are in this for two reasons: fame and glory, and an attempt to make a living. The fame and glory comes from their nationalistic goals. They are upholding the country's honor against both anti-Chinese forces like the pro-Tibet movement and larger forces like the United States."[104] However, Schneider argues nationalistic

[104]Bruce Schneier, "Chinese Cyber attacks: Myth or Menace?" www.schneier.com, www.schneier.com, July 2008, http://www.schneier.com/essay-227.htmlhttp://www.schneier.com/essay-227.html (accessed September 20, 2011).

hacking groups are dangerous because, although tolerated by the PRC, they are not regulated by the Chinese government and are more like rogue non-state actors.[105]

## Conclusion

No one recommends ignoring cyber threats, especially threats emanating from the PRC. However, it is important to understand where threats are coming from and how to define them. Currently, no United States government, military, or international cyber definitions exist, which means cyber espionage or spying is often portrayed as a cyber attack. China and the United States have differing definitions for acts in cyberspace and likely varied levels of tolerance for events in cyberspace. Technologically advanced countries like the United States have more to lose from lesser developed countries merely spying and stealing information. Many victims of cyber intrusions blame the PRC or PLA. However, security analysts acknowledge proving the location of the server and knowing how information was routed does not verify an enemy's location.

While cyber technology continues to advance and the awareness of PLA cyber capabilities grow, security experts and politicians play an enormous role in the level of attention cyberspace and the Chinese cyber threat receive. If evidence shows the PRC has the ability to commit cyber espionage but not cyber attacks, their intent could change overtime. Even if cyber intrusions cannot be traced back to the perpetrator, preparation must be taken to thwart them. Joel Brenner warns, "Intentions can change on a dime but capabilities and defenses cannot. A nation that puts its faith in a potential adversary's benign intentions rather than its own strength and capabilities is a nation that is psychologically and practically incapable of defending itself."[106] Brenner makes a valid point that the cyber security infrastructure must be in place to thwart current and future cyber threats. Intelligence officers examine not only the enemy's most likely course of action but the most dangerous course of action as well. A cyber threat from the

---

[105]Schneier, "Chinese Cyber attacks: Myth or Menace?"

[106] Joel Brenner, 156.

PRC, although exaggerated, does exist and our government and military need to take measures to deter and counter cyber threats.

Despite only examining open source reporting that the PLA has the ability to conduct a denial-of-service attack on the Falun Gong, one can make the conceptual leap that the PLA wants the public to see they have some level of cyber capability. Additionally, through writings, the PLA demonstrates they have a desire to conduct offensive cyber operations. Moreover, General Dai began writing about war in cyberspace and IW over ten years ago. Today, the PLA, like the United States have increased their cyber capabilities over the last decade. The development of a cyber blue team to secure their own networks from cyber threats and the continued emphasis on the concept of informatization are evidence that the cyber domain is a priority to the PRC.

China's lack of transparency and their incessant pleas that they are not responsible for cyber intrusions cause speculation and worry in the United States.[107] According to General Cartwright's definition of cyber attack, if networks were victims of cyber attacks their computers would be unusable. This is clearly not the case and reconnaissance via computer to spot vulnerabilities before the first battle is more than likely what the Chinese are doing. This method of reconnaissance fits well with the Eastern military stratagem of winning before the first battle.[108] Lack of transparency in the PRC and in the PLA's doctrine or rules and regulations require the United States government to remain vigilant. Working towards understanding links between hacker organizations and the PRC is paramount to understanding China's intentions. Conversely, the PRC has a large internal cyber threat to worry about emanating from their technically sophisticated and growing youth bulge.

In conclusion, accusations that the Chinese are a cyber threat appear to be growing right alongside with increased reporting of cyber threats. This increase in global reporting is likely the result of

---

[107] Timothy L. Thomas, "China's Electronic Long-Range Reconnaissance," 54.

[108] Ibid., 47.

growing Internet use increasing the number of vulnerable users as well as an increase in hackers with access to cheap hacker toolkits. Hackers, China's internal security threat, are likely their first and foremost priority. However, China has worked hard over the last ten years to grow almost every aspect of their military. Moreover, their growth in informatization and IW militias should not be overlooked or discounted. If the PRC's exaggerated cyber threat is the catalyst to get DoD to spend billions in developing offensive and defensive cyber systems and publish doctrine and policy, then maybe an exaggerated threat has a positive side.

# BIBLIOGRAPHY


**Books**

Brenner, Joel. America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. New York: Penguin Press, 2011.

Krepinevich, Andrew. 7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century. New York: Random House, 2009.

Kissinger,Henry. *On China*. New York: Penguin Press, 2011.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America.* Panama: Pan American Publishing Company, 2006.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* California: RAND Corporation, 2007.

———. *Cyberdeterrence and Cyberwar*. California: RAND Corporation, 2009.

Starr, Stuart H. "Toward a Preliminary Theory of Cyberpower,"*Cyberpower and National Security*. *Cyberpower and National Security* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Washington D.C.: NDU Press, 2009.

Sun Tzu. *Sun Tzu: The Art of Warfare*, ed. and trans. Samuel B. Griffith. New York: Oxford University Press, 1971.

Thomas, Timothy L. *Decoding the Virtual Dragon*. Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

———. *Dragon Bytes: Chinese Information-War, Theory, and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

———. "Nation State Cyber Strategies: Examples from China and Russia," Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington D.C.: National Defense University Press, 2009.

———. The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force. Fort Leavenworth, KS: Foreign Military Studies Office, 2009.

Wasserstrom, Jeffrey N. *China in the 21st Century: What Everyone Needs to Know*. New York: Oxford University Press, 2010.

**Journal Articles**

Alexander, Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* 5, no. 2, June 2011: 3-12.

Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges* 7, no. 2 (Winter 2011): 81-105.

Cheng, Dean. "Chinese Views on Deterrence." *Joint Forces Quarterly* 60, no. 1 (January 2011): 92-94.

Fritz, Joel. "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala* 8, no. 1, (2008): 28-80.

Goel, Sanjay. "Cyberwarfare: Connecting the Dots in Cyber Intelligence." *Communications of the ACM* 54, no. 8, (2011): 132-40.

Inkster, Nigel. "China in Cyberspace." *Survival* 52, no. 4 (August/September 2010): 55-66.

Lan, Tang and Zhang Xin. “Can Cyber Deterrence Work?” *Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway*, Edited by Andrew Nagorski, East West Institute. April 2010 www.ewi.info/system/files/CyberDeterrenceWeb.pdf (accessed on December 24, 2011): 1-2.

Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010. https://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed August 4, 2011).

———. “The Pentagon’s Cyberstrategy, One Year Later.” *Foreign Affairs.com,* September 28, 2011. http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later (accessed September 30, 2011).

Manson, George Patterson. "Cyberwar: The United States and China Prepare for the Next Generation of Conflict." *Comparative Strategy* 30, no. 2 (April-June 2011): 121-133.

Miller Robert A., Daniel T. Kuehl and Irving Lachow. "Cyber War: Issues in Attack and Defense." *Joint Forces Quarterly* 61, 2nd Quarter (2011): 18-31.

Ophardt, Jonathan A. “Cyberwarfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow‘s Battlefield.”*Duke Law and Technology Review (*February 2010). http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html#B19 (accessed November 25, 2011).

Ownby, David. “The Falun Gong in the New World.” *European Journal of East Asian Studies* 2, no. 2 (2003): 303-320.

Thomas, Timothy L. "China's Electronic Long-Range Reconnaissance." *Military Review*, 88, no. 6 (November-December 2008): 47-54.

———. “Google Confronts China’s ‘Three Warfares,” *Parameters*, Summer 2010. http://www.carlisle.army.mil/USAWC/parameters/Articles/2010summer/Thomas.pdf (accessed August 15, 2011).

**Monographs and Theses**

Are, David C. “When does a “Hacker” Become and “Attacker?” Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, 1999.

Beidleman, Scott W. “Defining and Deterring Cyber War.” Research paper, United States Army War College, 2009.

Oakley, John. “Cyber Warfare: China’s Strategy to Dominate in Cyber Space.” Master’s Thesis, United States Army Command and General Staff College, 2011.

**Government Documents**

Bartholomew, Carolyn. *2011 Report to Congress of the US- China Economic and Security Review Commission*. Washington, DC: Government Printing Office, November 2011.

"Chinese Cyber-Attacks on Google Further Highlights Need to Improve American Cybersecurity Infrastructure: Senate Commerce, Science, and Transportation Committee News Release." Congressional Documents and Publications, January 13, 2010.http://www.proquest.com (accessed August 27, 2011).

Office of the Secretary of Defense. “Military and Security Developments Involving the People’s Republic of China 2010,” 2010. http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf (accessed November 26, 2011).

Timperlake, Edward. “Testimony on Cyber-attacks, Espionage, and Technology Transfers to the People’s Republic of China.” *Foreign Affairs Committee, United States House of Representatives*, published April 15, 2011. http://www.strategycenter.net/research/pubID.242/pub_detail.asp (accessed November 25, 2011).

US Army Training and Doctrine Command (TRADOC). Army Doctrinal Publication (ADP) 3-0, *Unified Land Operations.* Washington D.C.: Government Printing Office, October 10, 2011.

———. Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington, DC: Government Printing Office, 2003.

———. Pamphlet 525-7-8, *Cyber Space Operations Concept Capability Plan 2016-2028*. Washington, DC: Government Printing Office, 2010.

———. Field Manual (FM) 1-02, *Operational Terms and Graphics.* Washington, DC: Government Printing Office, 2004.

US Department of Defense. “China: Information-System-Based Network Operation Theories.” January 29, 2011. https://www.opensource.gov/portal/server.pt/gateway (accessed September 4, 2011).

———. "Department of Defense Strategy for Operating in Cyberspace, July 2011.” http://www.defense.gov/news/d20110714cyber.pdf (accessed August 4, 2011).

———. Joint Publication (JP) 1-02: Department of Defense Dictionary of Military and Associated Terms. Washington D.C.: Government Printing Office, November 15, 2011.

———. *Joint Publication (JP) 3-13: Information Operations*. Washington D.C.: Government Printing Office, February 13, 2006.

———. “Military and Security Developments Involving the People’s Republic of China, 2011.” http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf (accessed September 4, 2011).

US Department of Education. “ National Center for Education Statistics”. 2011. *Digest of Education Statistics*, 2010, http://nces.ed.gov/fastfacts/display.asp?id=37 (accessed November 25, 2011).

**Electronic Documents**

Alperovitch, Dmitri. “Revealed: Operation Shady RAT,” *McAfee.com*, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed 25 November 2011).

Beidel, Eric and Stew Magnuson. “Government Military Face Severe Shortage of Cybersecurity Experts.” *nationaldefensemagazine.org*, August 2011. http://www.nationaldefensemagazine.org /archive/2011/August/Pages/Government,

MilitaryFaceSevereShortageOfCybersecurityExperts.aspx (accessed August 31, 2011).

Breeden, John II. “China Provides Smoking Gun against Itself in Cyberattacks,” *fcw.com,* August 29, 2011. http://fcw.com/Articles/2011/08/26/China-US-cyberattacks-smoking-gun.aspx?sc_lang=en&Page=1 (accessed October 10, 2011).

Cartwright, James. “*Joint Terminology for Cyberspace Operations,*” November 2010. http://www.nsci-va.org/CyberReferenceLib/2010-11 Joint%20Terminology%20for%20Cyberspace %20 Operations.pdf (accessed November 28, 2011).

“DoD could spend $13 billion on cyber security by fiscal year 2016.”*infosecurity.com*, October 20, 2011.http://www.infosecurity-magazine.com/view/21488/dod-could-spend-13-billion-on-cybersecurity-by-fiscal-year-2016/ (accessed October 29, 2011).

"DoD Cybersecurity Spending: Where is the Beef?" *defenseindustrydaily.com*, June 14, 2011. www.defenseindustrydaily.com/cyber-security-department-defense-spending-06882/ (accessed September 29, 2011).

Forbes, Randy J., Congressman. Press Release, "In Face of Chinese Cyber Attacks, US is Losing" April 21, 2011. http://forbes.house.gov/News/DocumentSingle.aspx?DocumentID=181560 (accessed October 5, 2011).

Hersh, Seymour M. "The Online Threat. Should we be Worried about a Cyber War?" *projectworldawareness.com*, December 11, 2011. http://www.projectworldawareness.com /2010/12/the-online-threat-should-we-be-worried-about-a-cyber-war/ (accessed December 23, 2011).

Grauman, Brigid. "Cyber-Security: The Vexed Question of Global Rule." 2012. http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf (accessed February 11, 2012).

Internet World Stats: Usage and Population Statistics, http://www.internetworldstats.com/stats14.htm (accessed September 20, 2011).

Isenberg, David."Electronic Pearl Harbor? More Hype than Threat." *Cato Institute Daily*.http://www.cato.org/pub_display.php?pub_id=4841 (accessed August 24, 2011).

Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Northrup Grumman Corporation, October 9, 2009. http;//handle.dtic.mil/100.2/ADA509000 (accessed October 10, 2011).

Lewis, Leo. "China's Blue Army of 30 Computer Experts could Deploy Cyber Warfare on Foreign Powers." *The australian.com*, May 27, 2011. http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826 (accessed December 2, 2011).

McLaughlin, Matt. "Building a Force for Fighting in Cyberspace," *Fed Tech Magazine.com*, August 2011. http://www.fedtechmagazine.com/print_friendly.asp?item_id=1064 (accessed September 8, 2011).

Rogin, Josh. "The Top Ten Chinese Cyber Attacks that we Know of." *foreignpolicy.com* , January 22, 2010.http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that we_know_of (accessed November 24, 2011).

Schneier, Bruce. "Chinese Cyber attacks: Myth or Menace?" *schneier.com*, July 2008. http://www.schneier.com/essay- 227.html (accessed September 20, 2011).

———. "Threat of "Cyberwar" Has Been Hugely Hyped." *schneier.com*, July 7, 2010. http://www.schneier.com/essay-320.html (accessed December 23, 2011).

Serrano, Alfonso F. "Cyber Crime Pays: A $114 Billion Industry." *The Fiscal Times*, September 14, 2011. http://www.thefiscaltimes.com/Articles/2011/09/14/Cyber-Crime-Pays-A-114-Billion-Industry.aspx#page1 (assessed November 14, 2011).

Stokes, Mark A., Jenny Lin and L.C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." *Project 2049 Institute*, November 11, 2011. https://project2049.net/publications.html (accessed November 15, 2011).

Symantec Corporation. "Symantec Global Internet Security Threat Report Trends for 2009." 15, no.1, April 2010. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_ security_ threat_report_xv_04-2010.en-us.pdf (accessed December 26, 2011).

Thompson, Loren."Cyberwarfare May be a Bust for Many Defense Contractors." *forbes.com*, May 9, 2011. www.forbes.com/sites/beltway/2011/05/09-washingtons-cyberwarfare-boom-loses-its-allure/ (accessed October 29, 2011).

Xu, Ting. "China and the United States: Hacking Away at Cyber Warfare." *Asia Pacific Bulletin* 135, November 1, 2011. http://www.eastwestcenter.org/publications/china-and-united-states-hacking-away-cyber-warfare (accessed December 27, 2011).

**Articles**

Jackson, William. "When is a Cyberattack not a Cyberattack? Most of the Time." *Federal Computer Week*, August 8, 2011.

Zyskowski, John. "Advanced persistent threats: Be fearful but keep perspective." *Federal Computer Week*, August 8, 2011.